Probability Reminder

Cryptography and Protocols
Andrei Bulatov

样本空间

Sample Space and Outcomes

- Experiments and outcomes
- Sample space is the set of all possible outcomes
- Examples
    - flipping a coin Ω = {heads, tails}
    - flipping a pair of coins Ω = {HH, HT, TH, TT}
    - horse race (7 horses) Ω = {all 7! permutations of (1,2,3,4,5,6,7)}

      扔 两个骰子
    - tossing two dice Ω = {11,12, … , 66}
    - flipping k coins $\Omega = \{0,1\}^k$

Events

- Event is any subset of the sample space
- Examples
  - any outcome is an event (a 1-element subset)
  - getting even number of heads when flipping a pair of coins
  - horse no. 4 came second
  - getting at least one 3 when tossing two dice
- Algebra of events
  - union of events $A \cup B$
  - intersection $A \cap B$
  - complement $\bar{A}$
  - mutually exclusive events $A \cap B = \emptyset$ A B不相交

Probability: Case of Equally Likely Outcomes

- If all the outcomes are equally likely, then the probability of event A equals

$$\Pr[A] = \frac{m}{n}$$

where m is the number of outcomes in A, and n the total number of outcomes

- Examples
  - getting even number of heads when flipping a pair of coins
  - horse no. 4 came second
  - getting at least one 3 when tossing two dice

1. Flipping a pair of coins

$\Omega = \{HH, HT, TH, TT\}$

$n = |\Omega| = 4$

event A : even # of heads

$A = \{HH, TT\}$

$m = |A| = 2$

$Pr[A] = \frac{m}{n} = \frac{2}{4} = \frac{1}{2}$

2. Horse race

$\Omega = \{\text{permutations of 7 horses}\}$

$n = |\Omega| = 7! = 7 \cdot 6 \cdot \cdots \cdot 1$

A = horse # 4 comes 2nd = {permutations of 6 horses}

$m = |A| = 6!$

$Pr[A] = \frac{m}{n} = \frac{6!}{7!} = \frac{1}{7}$

3. Getting a 3 when tossing 2 dice

$\Omega = \{11, 12, \cdots, 66\}$

$n = |\Omega| = 36$

$A = \{31, 32, 33, 34, 35, 36, 13, 23, \cancel{33}, 43, 53, 63\}$

$m = |A| = 11 \qquad Pr[A] = \frac{11}{36}$

Distribution

- In the general case each outcome a is associated with probability it happens Pr[{a}] , or just Pr[a]. The collection of these numbers is called a distribution
- A distribution must satisfy the property

$$\sum_{a\in\Omega} \Pr[a] = 1$$

- Examples
  - uniform distribution: all outcomes are equally likely
  - important uniform distribution, U_n selecting an n-bit string
  - crooked die: Pr[1] = 1/3, Pr[2] = Pr[3] = Pr[4] = Pr[5] = 1/6, Pr[6] = 0 歪骰子

General Probability

- Given a probability distribution over Ω we can define the probability of any event as follows:

$$\Pr[A] = \sum_{a \in A} \Pr[a]$$

- Examples

  - What is the probability to get an even number tossing a crooked die:

  Pr[1] = 1/3, Pr[2] = Pr[3] = Pr[4] = Pr[5] = 1/6, Pr[6] = 0

Crooked die

A even number when rolling the die.

$A = \{2, 4, 6\}$

$\Pr[A] = \Pr[2] + \Pr[4] + \Pr[6]$

$= \frac{1}{6} + \frac{1}{6} + 0$

$= \frac{1}{3}$

Properties of Probability

- $\Pr[\bar{A}] = 1 - \Pr[A]$
- If $A \subseteq B$ then $\Pr[A] \leq \Pr[B]$
- $\Pr[A \cup B] = \Pr[A] + \Pr[B] - \Pr[AB]$
- Examples
  - what is the probability to get at least one heads flipping 33 coins?

- Union Bound: union 的上限

  For any events A and B $\Pr[A \cup B] \leq \Pr[A] + \Pr[B]$
- Consider U_3 and estimate the probability that a string starts with 1 or ends with 1

  U_3 : select an 3-bit string

- what is the probability to get at least one heads flipping 33 coins?

A getting at least 1 heads

$\bar{A}$ getting no heads

$\bar{A} = \{TT \cdots T\}$ (33 times)

$|\bar{A}| = 1 \qquad |\Omega| = 2^{33}$

$Pr[\bar{A}] = \frac{1}{2^{33}}$

$Pr[A] = 1 - Pr[\bar{A}] = 1 - \frac{1}{2^{33}}$

Conditional Probability

- The probability of event A conditional on event B is the probability that A happened if it is known that B happened
- Example ↳ A based on B，也就是说，此时B为总集.

Toss two dice. What is the probability that the sum of the two dice is 8 if the first die is 3?

A: the sum is 8

B: the 1st die 3

B = {31, 32, 33, 34, 35, 36}

the conditional probability of A given B : $\frac{1}{6}$

Conditional Probability

- Probability of A conditional on B is denoted Pr[A | B]
- This probability equals

$$\Pr[A|B] = \frac{\Pr[A \cap B]}{\Pr[B]}$$

- Multiplication rule: $\Pr[A \cap B] = \Pr[A|B] \cdot \Pr[B]$

Independent Events A, B 互不相关

- Events A,B are independent if Pr[A|B] = Pr[A] and Pr[B|A] = Pr[B]
- Examples:

  - flipping two coins A = {first coin comes up heads} , B = {second coin comes up heads} Independent

  - tossing two dice A = {sum of the dice is 3}, B = {first die is even} not independent

$$Pr[A|B] = \frac{Pr[A \cap B]}{Pr[B]}$$

$B = \{21 \dots 26, 41 \dots 46, 61 \dots 66\}$

$Pr[B] = \frac{18}{36} = \frac{1}{2}$

$A \cap B = \{21\}$

$Pr[A \cap B] = \frac{1}{36}$

$Pr[A|B] = \frac{1/36}{1/2} = \frac{1}{18}$

$Pr[A] = \frac{2}{36} = \frac{1}{18}$

$A = \{12, 21\}$

Random Variables

- A random variable is a function of the outcomes
- Formally: $X : \Omega \to R$ (real numbers) Ω是总集
- Discrete random variable: $X : \Omega \to \{x_1, \dots, x_k\}$
- Examples:
  - sum of two dice
  - number of heads
  - lifetime of an electric bulb 电灯泡
- Sum and product of random variables X + Y, XY, aX

X: sum of #'s on 2 dice

$V = \{2, 3, 4, \dots, 12\}$ (11 possible #'s)

$Pr[x=2] = \frac{1}{36}$ only outcome: 11

$Pr[X=3] = \frac{2}{36} = \frac{1}{18}$ 2 outcomes: 12 21

Distribution of Random Variable

- Let X be a discrete random variable with values $x_1, \dots, x_k$
Then its distribution is a collection of numbers $p_1, \dots, p_k$
such that $\Pr[X = x_i] = p_i$
- Note: $\sum_{i=1}^{k} p_i = 1$
- Examples:

  - uniform distribution : all probabilities are equal, e.g. random variable X with values 0 = heads and 1 = tails when flipping a coin (Bernoulli random variable)

  伯努利 随机变量

  - sum of two dice is not uniform

Distribution of Random Variable: More Examples

- Examples:

  - number of heads when flipping $\overset{u_k}{k}$ coins

$k=3$ $\quad Pr[N=1] = \frac{3}{8}$ $\quad$ 100 010 001

$Pr[N=3] = \frac{1}{8}$ $\quad$ 111

  - more general – binomial random variable N: the number of successes in k repetitions of the same experiment (*independent*!); each repetition is successful with probability p

0 – failure

1 – success

Binomial Random Variable 二项式随机变量

- Suppose that the outcomes of the experiment are bits 0 and 1

  1 happens with probability p
- The probability of a particular string with m 1s: $p^m(1-p)^{k-m}$
- The probability of a string with m 1s:

$$\Pr[N = m] = \binom{k}{m} p^m (1-p)^{k-m}$$

- Let N_i be the random variable that equals the number of successes in the i'th experiment. Then

$$N = N_1 + \cdots + N_k$$

Expectation

- The expectation of a random variable is its `mean' value
- Formally, if V is the set of possible values of a random variable X, then

$$\mathrm{E}(X) = \sum_{v \in V} v \cdot \Pr[X = v]$$

- Properties of expectation:
  - let X be a random variable, let a be a number then

    $$\mathrm{E}(aX) = a \cdot \mathrm{E}(X)$$

  - let X and Y be random variables then

    $$\mathrm{E}(X + Y) = \mathrm{E}(X) + E(Y)$$

Expectation (cntd)

- Example

  Lottery: 1000000 tickets, 4 tickets win $1000000, 5 tickets win $100000, 5000 tickets win $1000. What is the average win?

X : the amount won

V : {1000000, 100000, 1000, 0}

$\Pr[X=10^6] = \frac{4}{10^6}$

$\Pr[X=10^5] = \frac{5}{10^6}$

$\Pr[X=1000] = \frac{5000}{10^6} = \frac{1}{200}$

$\Pr[X=0] =$ the rest

$E(X) = 10^6 \cdot \Pr[X=10^6] + 10^5 \cdot \Pr[X=10^5] + 1000 \cdot \Pr[X=1000] + 0 \cdot \Pr[X=0]$

$= 10^6 \cdot \frac{4}{10^6} + 10^5 \cdot \frac{5}{10^6} + 1000 \cdot \frac{5}{1000}$

$= 4 + 0.5 + 5 = 9.5$

- Expectation of Bernoulli random variable

  $\Pr[N=1] = p, \quad \Pr[N=0] = 1-p$

  $E(N) = p = 1 \cdot p + 0 \cdot (1-p) = p$

- Expectation of the binomial random variable (k trials):

  $E(N) = E(N_1 + \cdots + N_k) = E(N_1) + \cdots + E(N_k) = k \cdot p$

比如硬币一共投了6次，

则正面向上次数的期望值为 $6 \times \frac{1}{2} = 3$ 次

Independent Random Variables

- Random variables X and Y are independent if for any value v of X and any value w of Y the events $X = v$ and $Y = w$ are independent
- Example
  - flipping 2 coins, N and N_1 are not independent
  - flipping 2 coins, N_1 and N_2 are independent
- Properties of expectation
  - if X and Y are independent then $\mathrm{E}(XY) = \mathrm{E}(X) \cdot \mathrm{E}(Y)$

A= 投2枚硬币

X= 第一枚硬币正面朝上 $E(X) = \frac{1}{2}$

Y= 第二枚硬币正面朝上 $E(Y) = \frac{1}{2}$

XY= 两枚硬币都正面朝上 $E(XY) = \frac{1}{4}$

Birthday Paradox

- Suppose we have n people at a party. What is the probability some two of them have the same birthday?
- How many guests are needed so that this happens with considerable probability? Say, $\geq \frac{1}{2}$
- **Theorem**:

  Let $a_1, \ldots, a_n$ be outcomes of n independent trials of the same experiment with sample space Ω. If $n \geq 1.2 \cdot \sqrt{|\Omega|}$ then the probability that $a_i = a_j$ for some i, j is greater than $\frac{1}{2}$
- For birthdays $|\Omega| = 365$

两个人生日是同一天的机率$\geq \frac{1}{2}$的概率

(概率の概率)

Randomized Algorithms

- An algorithm that has access to random bits, that is, can flip coins, is called randomized
- The sample space associated with such an algorithm is the set of possible bit strings
- A random variable associated with it is, for instance, the running time

↳ break a crypto system by a chance.

↳ try to guess a password.